CORRECTED VERSION*

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00 — A1

(11) International Publication Number: WO 98/44676

(43) International Publication Date: 8 October 1998 (08.10.98)

(21) International Application Number: PCT/US98/05010

(22) International Filing Date: 12 March 1998 (12.03.98)

(30) Priority Data:
08/829,594 31 March 1997 (31.03.97) US

(71) Applicant: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95054 (US).

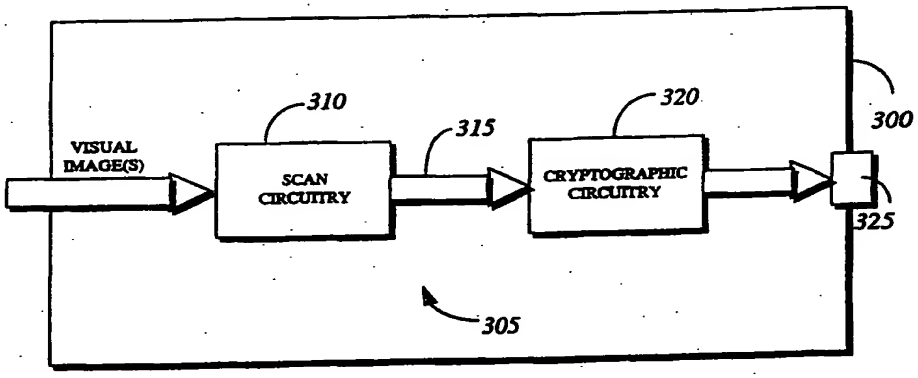
(72) Inventor: DAVIS, Derek; 4509 E. Desert Trumpet Road, Pheonix, AZ 85044 (US).

(74) Agents: TAYLOR, Edwin, H. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

(81) Designated States: AL, AM, AT, AT (Utility model), AU (Petty patent), AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
With amended claims.

(54) Title: A PERIPHERAL DEVICE PREVENTING POST-SCAN MODIFICATION



(57) Abstract

Both dedicated scanners and shared-resource scanners comprise a casing (300). The casing (300) protects the internal circuitry (305) from harmful contaminants and environmental conditions. The internal circuitry (305) includes scan circuitry (310) and cryptographic circuitry (320). The scan circuitry digitizes a visual image on a document to produce a data set (315). The data set (315) is routed to the cryptographic circuitry (320) within the casing (300) to produce a corresponding digital signature.. At least a digital signature is output by the output port (325).

EL594612728US

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon			PT	Portugal		
CN	China	KR	Republic of Korea	RO	Romania		
CU	Cuba	KZ	Kazakstan	RU	Russian Federation		
CZ	Czech Republic	LC	Saint Lucia	SD	Sudan		
DE	Germany	LI	Liechtenstein	SE	Sweden		
DK	Denmark	LK	Sri Lanka	SG	Singapore		
EE	Estonia	LR	Liberia				

A PERIPHERAL DEVICE PREVENTING POST-SCAN MODIFICATION

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the field of data security. More particularly, the present invention relates to a peripheral device that (i) converts visible images into digital data, and (ii) digitally signs the data to prevent its unauthorized modification.

2. Description of Art Related to the Invention

For many years, our society has maintained a paper-based, communicative infrastructure that relies on documents. Herein, a "document" is broadly defined as one or more pieces of paper of any physical dimension with visible images placed thereon. These visual images include alphanumeric characters associated with any language as well as symbols or drawings.

Documents have been widely used for a variety of situations. For example, documents can be used as "receipts" in order to provide a consumer with a record of goods or services purchased by the consumer. Sometimes, receipts are required to obtain a refund or credit for a prior purchase, to receive a reimbursement for work-related expenses, to recover damages from insurance companies, to support a claimed tax deduction, and other reasons.

As our paper-based, social infrastructure slowly transitions into an electronic-based, social infrastructure, it is contemplated that a temporary hybrid system, which supports a mixture of paper and electronic medium, may be necessary. This is due to the fact that there are certain situations where documents need to be processed in paper form. For example, it is believed that expense reports need to be filed with original signatures in order to obtain tax relief. As digital signatures become recognized as an acceptable alternative to handwritten signatures, electronic transmission of expense reports may become an acceptable practice.

Unfortunately, in the case of expense reports, other documents are usually required to accompany the expense report. These documents may include receipts for meals, lodging and transportation which are provided in a paper form. While we can expect that many receipts may migrate to an electronic format over the long term, some receipts may remain in paper form for an indefinite period of time. Thus, even if the expense report could be filed electronically, electronic-only handling of the entire expense report currently is not possible.

One possible solution to this problem is to digitally scan the receipts using a dedicated scanner to produce a data set, and to temporarily store the data set within a computer. Thereafter, the data set is transmitted with the electronic expense report. However, this creates an opportunity for illicit post-scan modification of the data set. Illicit post-scan modification would expose businesses to the danger of exaggerated reimbursement requests, and would also expose local, state and/or federal legislatures to claims of exaggerated tax deductions by businesses.

Thus, it would also be advantageous to create a system and method which discourages illicit post-scan modifications by providing a reliable mechanism to easily detect such modification.

SUMMARY OF THE INVENTION

The present invention is related to a system and method for preventing unauthorized modification of a data set after being output from a peripheral device. After digitizing visual images of a document, a digital signature based on the data set is produced within the peripheral device. Preferably, this digital signature is output along with the data set to provide a mechanism, used to check at its destination, whether the data set has experienced post-scan modification.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is a first embodiment of an electronic system including a dedicated scanner capable of digitally signing a data set.

Figure 2 is a second embodiment of an electronic system including a shared-resource scanner coupled to a network, the scanner producing a digital signature based on the data set before its transmission to a destination.

Figure 3 is an embodiment of the scanner employing cryptographic circuitry capable of producing the digital signature.

Figure 4 is an embodiment of a cryptographic processor being at least a portion of the cryptographic circuitry of Figure 3.

Figure 5 is an illustrative block diagram of the operations performed by the scanner to prevent post-scan modification.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention generally relates to a peripheral device that discourages unauthorized modification of the content of a data set. More specifically, the peripheral device involves a scanner which produces a digital representation that is difficult to illicitly modify without subsequent detection of such modification. While the description focuses on a scanner, other alternative embodiments of the peripheral device are contemplated such as a facsimile machine.

Herein, certain details are set forth in order to provide a thorough understanding of the present invention. Without deviating from its spirit and scope, the present invention may be practiced through many different embodiments, other than those embodiments illustrated. In addition, well-known circuits, elements and the like may not set forth in detail in order to avoid unnecessarily obscuring the present invention.

In the detailed description, a number of terms are frequently used to describe certain characteristics or qualities which are defined herein. A "key" is an encoding and/or decoding parameter used by symmetric key cryptographic functions such as Data Encryption Standard (DES) or public-key cryptographic functions such as Rivest Shamir Adleman (RSA). A "data set" is defined as digitized data corresponding to a scanned document. A "digital certificate" is defined as digital information (e.g., a public key) cryptographically bound by a private key by a widely known "trusted" authority. A trusted authority may include, but is not limited or restricted to a bank, governmental entity, trade association, original equipment manufacturer, security department, or any person or entity in a position of trust to guarantee or sponsor the digital certificate. A "digital signature" involves application of a cryptographic signing function (e.g., Digital Signaturing Algorithm "DSA") to a data set (or its corresponding hash value) in order to ensure its integrity.

Referring to Figure 1, a perspective view of a first embodiment of the electronic system 100 utilizing the present invention is shown. The electronic system 100 features a computer 110 interconnected to a number of peripheral devices 120. Computer 110 may be interconnected to a network such as a dedicated local area network (LAN) or a wide area network (WAN) such as the Internet. This

allows computer 110 to electronically communicate with other computers in order to upload or download data sets.

As shown, the peripheral devices 120 may include a data input source (e.g., a keyboard, a numeric pad, a cursor control device, etc.) 125 and an optical scanner 130. Normally, coupled to a port located on the backside of computer 110 (e.g., a serial, parallel, Universal Serial Bus port, etc.), scanner 130 may be a desktop scanner constructed as a flatbed scanner, or as shown, a scanner having an automatic feed mechanism (e.g., a rotated roller) to assist in scanning of a document 135. As an alternative embodiment (not shown), scanner 130 may be constructed as a hand-held scanner. Unlike the desktop scanner, the hand-held scanner requires active participation by the user to adjust the scanner or document in order to produce a data set for the document.

Referring now to Figure 2, a perspective view of a second embodiment of the electronic system 200 utilizing the present invention is shown. Electronic system 200 is a shared-resource scanner 210 coupled to a network (e.g., a local area network "LAN" or a wide area network "WAN") 220. For illustrative purposes, shared-resource scanner 210 is shown as a flatbed scanner including a scanning platform 230 upon which a document 240 is laid face-down with its visible image(s) facing the scanning platform 230. Document 240 is scanned by moving scanning platform 230 along a generally horizontal direction as indicated by arrow 250 or by moving the scanning device along that generally horizontal direction. The resulting data set, a digital representation of the document, is routed to a targeted source 260 through network 220. It is contemplated that shared-resource scanner 210 may include any other type of scanner construction.

Referring now to Figure 3, both dedicated scanners and shared-resource scanners comprise a casing 300. The casing 300 protects internal circuitry 305 from harmful contaminants and environmental conditions. Internal circuitry 305 includes scan circuitry 310 and cryptographic circuitry 320. Well-known in the art, the scan circuitry 310 converts visual image(s) placed on a document into a data set 315 featuring digital representations of the visual image(s). Normally, these digital representations possess certain characteristics (e.g., size, resolution, contrast, etc.) substantially similar to the visual image(s). Unlike conventional scanners which subsequently route digitized data to a computer or a storage device, within the present invention, data set 315 is routed to cryptographic circuitry 320 within casing

300.

The cryptographic circuitry 320 performs cryptographic operations, such as producing a digital signature from the input data set 315, and outputs at least the digital signature and data set through an output port 325. One embodiment of this cryptographic circuitry 320 includes a cryptographic processor 400 implemented with an interface 405, a processing unit 410 and an internal memory 415 as shown in Figure 4. Interface 405 receives data set 315 (of Figure 3) and appropriately places the data onto an internal bus 420, which is coupled to interface 405, processing unit 410 and internal memory 415. Processing unit 400 is configured to access stored information from internal memory 415 in order to process data set 315 and produce a digital signature. The digital signature, and typically the data set, would be output from interface 405, or possibly another interface (not shown), to external circuitry responsible for transmission to a targeted destination. This destination may include a dedicated computer storage device or any device connected to a network.

Internal memory 415 contains a key pair, namely a public key (PUKS) 425_1 and a private key (PRKS) 425_2. The private key (PRKS) is used to produce digital signatures. The public and private keys 425_1 and 425_2 may be unique to each particular scanner, or may be universally implemented into all scanners if this lesser type of protection is acceptable. Internal memory 415 may further contain (i) one or more shared keys to support symmetric key cryptography, and/or (ii) one or more digital certificates. Examples of a digital certificate that may be contained within internal memory 415 include at least a public key associated with the scanner (PUKS) encrypted with a private key of a trusted authority (PRKTA) whose public key (PUKTA) is pre-loaded or well-known and widely available.

It is contemplated, however, that there are other embodiments for cryptographic circuitry 320. One embodiment may include cryptographic processor 400 connected to memory, external to processor 400 but still within the casing 300 via one or more communication lines, in lieu of implementing internal memory 415 within cryptographic processor 400 as shown. Preferably, but not necessary, the communication lines would be "secure," with communications over the communication lines encrypted or protected through any other cryptographic operation.

Another embodiment of cryptographic circuitry 320 includes logic circuitry,

other than a processor, to produce the digital signature. Such logic circuitry may include, but is not limited or restricted to, a state machine configured to digitally sign input information, a micro-controller executing a cryptographic signing function, or any other hardware and software responsible for digitally signing a data set to create a digital signature.

Referring now to Figure 5, a block diagram featuring the internal operations of the peripheral device (e.g., optical scanner) of Figures 1-2 is shown. These internal operations are performed independent of its selected hardware implementation. Upon positioning the document on a scanning table or in a roller mechanism and placing the scanner into an operational state, each visual image is converted by scan circuitry into a corresponding digital representation of the image. Collectively, these digital representations form a data set 510. As shown, data set 510 undergoes a one-way hash function to produce a hash value 520 of a fixed bit length, normally smaller in size than data set 510.

Hash value 520 is digitally signed with the private key of the scanner (PRKS) to produce a digital signature 530. The private key (PRKS) may be unique to this scanner or commonly shared by a number of scanners. After digital signature 530 is produced within scanner 500, at least the digital signature 530 and the data set 510 are transmitted to a targeted destination 560 (e.g., a computer) for storage or use. Data set 510 may be transmitted in a non-encrypted format (as shown) or may be encrypted before transmission to its destination. Likewise, as represented by dotted lines, a digital certificate 550, including the public key (PUKS) of the scanner signed with a private key (PRKTA) of a remotely located trusted authority 540 using a public-key cryptographic function (e.g., RSA or DSA), may accompany the data set 510 and digital signature 530. Digital certificate 550 would be necessary if the public key (PUKS) of the scanner 500 is not widely available or was not somehow accessible (e.g., already pre-loaded) by targeted destination 560.

Upon receiving the digital bit stream from the scanner, if the digital certificate 550 is provided, targeted destination 560 initially decrypts digital certificate 550 using the public key of the trusted authority (PUKTA). The public key of the trusted authority (PUKTA) is available by previously storing PUKTA within targeted destination 560 or by loading PUKTA as needed. Such decryption allows targeted destination 560 to obtain access to the public key (PUKS) of scanner 500.

Once the targeted destination 560 has access to the public key of the scanner, either from decrypting digital certificate 550 or retrieving the previously loaded public key from memory within targeted destination 560, it decrypts digital signature 530 to obtain hash value 520. Prior, concurrent or subsequent to this operation, data set 510 undergoes a hashing operation utilizing the same hash function as used in the scanner 500. This hashing operation produces a comparison hash value 570. The comparison hash value 570 is compared to hash value 520. If these hash values 520 and 570 are identical, no modification of the data has been performed. However, if these hash values 520 and 570 differ, illicit post-scan modification of the data set has been performed or corruption occurred.

Alternatively, it is contemplated that a hash function may not be used to produce the digital signature 530. Instead, the data set 510 in its entirety is digitally signed. Thus, validation is conducted through comparison of the transmitted data set with the data set retrieved from digital signature 530.

Of course, the invention described herein may be designed in many different methods and using many different configurations. While the present invention has been described in terms of various embodiments, other embodiments may come to mind to those skilled in the art without departing from the spirit and scope of the present invention. The invention should, therefore, be measured in terms of the claims which follows.

CLAIMS

What is claimed is:

1. A method for preventing unauthorized modification of a data set after being output from a peripheral device, the method comprising the steps of:

producing a digital signature based on the data set within the peripheral device; and

outputting at least the digital signature from the peripheral device.

2. The method of claim 1, wherein prior to producing step, the method comprises the step of converting a plurality of visual images on a document into the data set.

3. The method of claim 1, wherein the peripheral device is a scanner.

4. The method of claim 3, wherein the producing step includes the steps of:

receiving the data set as input for a hash function;

converting the data set into a hash value by executing the hash function; and

digitally signing the hash value with a private key associated with the scanner.

5. The method of claim 3, wherein the producing step includes the step of digitally signing the data set with a private key associated with the scanner.

6. The method of claim 3, wherein the outputting step includes the step of providing both the data set and the digital signature.

7. The method of claim 1, wherein prior to the outputting step, the method further includes the step of producing a digital certificate, the digital certificate including a public key associated with the peripheral device encrypted to a private key of a trusted authority.

8. The method of claim 7, wherein the outputting step includes the step of providing the data set, the digital signature and the digital certificate.

9. The method of claim 7, wherein the outputting step includes the step of providing the digital certificate and the digital signature.

10. A scanner designed to prevent illicit modification of digital information after a document has been scanned, the scanner comprising:

scan circuitry capable of converting a plurality of visual images of the document into a data set; and

cryptographic circuitry coupled to the scan circuitry, the cryptographic circuitry produces a digital signature associated with the data set before the data set and the digital signature are output from the scanner.

11. The scanner of claim 10, wherein the cryptographic circuitry includes a cryptographic processor.

12. The scanner of claim 11, wherein the cryptographic processor includes

an internal bus;

an interface coupled to the internal bus, the interface receives the data set and places the data set onto the internal bus; and

a processing unit coupled to the internal bus, the processing unit performs at least one cryptographic operation on the data set in order to produce the digital signature.

13. The scanner of claim 12, wherein the cryptographic processor further includes internal memory to contain information needed for the processing unit to perform the at least one cryptographic operation.

14. The scanner of claim 13, wherein the information includes at least a private key associated with the scanner and at least one cryptographic program for execution by the processing unit.

15. The scanner of claim 12, wherein the cryptographic processor is coupled to an external memory element containing information needed by the processing unit to perform the at least one cryptographic operation.

16. A method for preventing illicit modification of digitized data produced by a scanner, the method comprising the steps of:

digitizing visual images placed on a document to create a data set;

converting the data set into a hash value;

digitally signing the hash value with a private key associated with the scanner to produce a digital signature; and

outputting at least the data set and the digital signature from the scanner.

17. The method of claim 16, wherein prior to the outputting step, the method for further comprising the step of receiving a digital certificate.

18. The method of claim 17, wherein the digital certificate includes a public key associated with the scanner digitally signed with a private key of a trusted authority.

AMENDED CLAIMS
[received by the International Bureau on 03 August 1998 (03.08.98); orignal claims 1-18 replaced by amended claims 1-14 (3 pages)]

1. A method for preventing unauthorized modification of a data set, the method comprising:

converting a plurality of visual images on a document into the data set by a peripheral device;

producing a digital signature based on the data set by the peripheral device; and

outputting at least the digital signature from the peripheral device.

2. The method of claim 1, wherein the peripheral device is a scanner.

3. The method of claim 1, wherein the producing of the digital signature includes:

receiving the data set as input for a hash function;

converting the data set into a hash value by executing the hash function; and

digitally signing the hash value with a private key associated with the scanner.

4. The method of claim 1, wherein the outputting of at least the digital signature includes providing both the data set and the digital signature.

5. The method of claim 1, wherein prior to the outputting of at least the digital signature, the method further includes producing a digital certificate, the digital certificate including a public key associated with the peripheral device encrypted to a private key of a trusted authority.

6. The method of claim 5, wherein the outputting of at least the digital signature includes providing the data set, the digital signature and the digital certificate.

7. A scanner designed to prevent illicit modification of digital information after a document has been scanned, the scanner comprising:

scan circuitry to convert a plurality of visual images of the document into a data set; and

cryptographic circuitry coupled to the scan circuitry, the cryptographic circuitry to produce a digital signature associated with the data set before the data set and the digital signature are output from the scanner.

8. The scanner of claim 7, wherein the cryptographic circuitry includes a cryptographic processor.

9. The scanner of claim 8, wherein the cryptographic processor includes

an internal bus;

an interface coupled to the internal bus, the interface to receive the data set and to place the data set onto the internal bus; and

a processing unit coupled to the internal bus, the processing unit to perform at least one cryptographic operation on the data set in order to produce the digital signature.

10. The scanner of claim 9, wherein the cryptographic processor further includes internal memory to contain at least a private key associated with the scanner and at least one cryptographic program for execution by the processing unit.

11. A method for preventing illicit modification of digitized data produced by a scanner, the method comprising:

digitizing visual images placed on a document to create a data set;

converting the data set into a hash value;

digitally signing the hash value with a private key associated with the scanner to produce a digital signature; and

outputting at least the data set and the digital signature from the scanner.

12. The method of claim 11, wherein prior to outputting the data set and the digital signature, the method further comprising receiving a digital certificate.

13. The method of claim 12, wherein the digital certificate includes a public key associated with the scanner digitally signed with a private key of a trusted authority.

14. A scanner designed to prevent illicit modification of digital information after a document has been scanned, the scanner comprising:

means for digitizing a plurality of visual images printed on the document to produce a data set; and

cryptographic means for producing a digital signature associated with the data set before the data set and the digital signature are output, the cryptographic means being coupled to the means for digitizing.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/05010

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04L 9/00
US CL : 380/25
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/25,4,9,23,30,49,50,51,54,55,59

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 5,291,243 A (HECKMAN et al) 01 March 1994, see abstract.	1 --- 2-18
X --- Y	US 5,530,755 A (PAILLES et al) 25 June 1996, see abstract.	1 --- 2-18
X --- Y	US 5,606,609 A (HOUSER et al) 25 February 1997, see abstract.	1 --- 2-18

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
14 MAY 1998

Date of mailing of the international search report
19 JUN 1998

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
BERNARR EARL GREGORY
Telephone No. (703) 306-4153

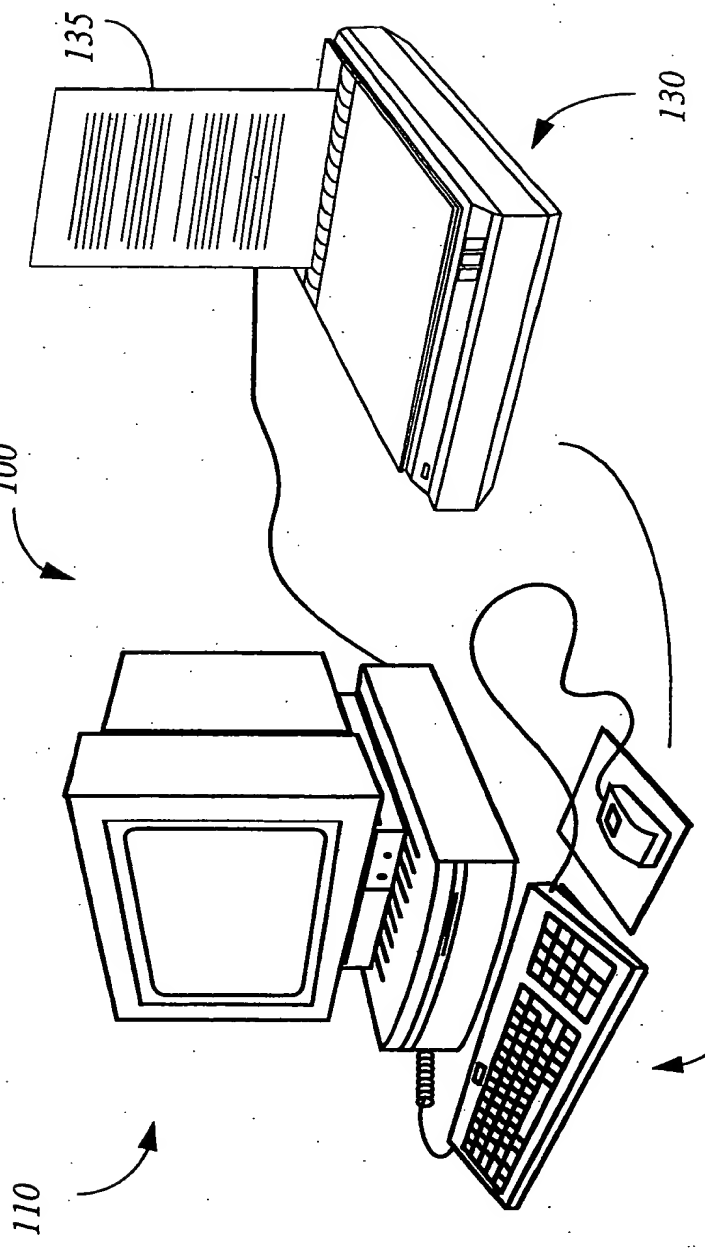


Figure 1

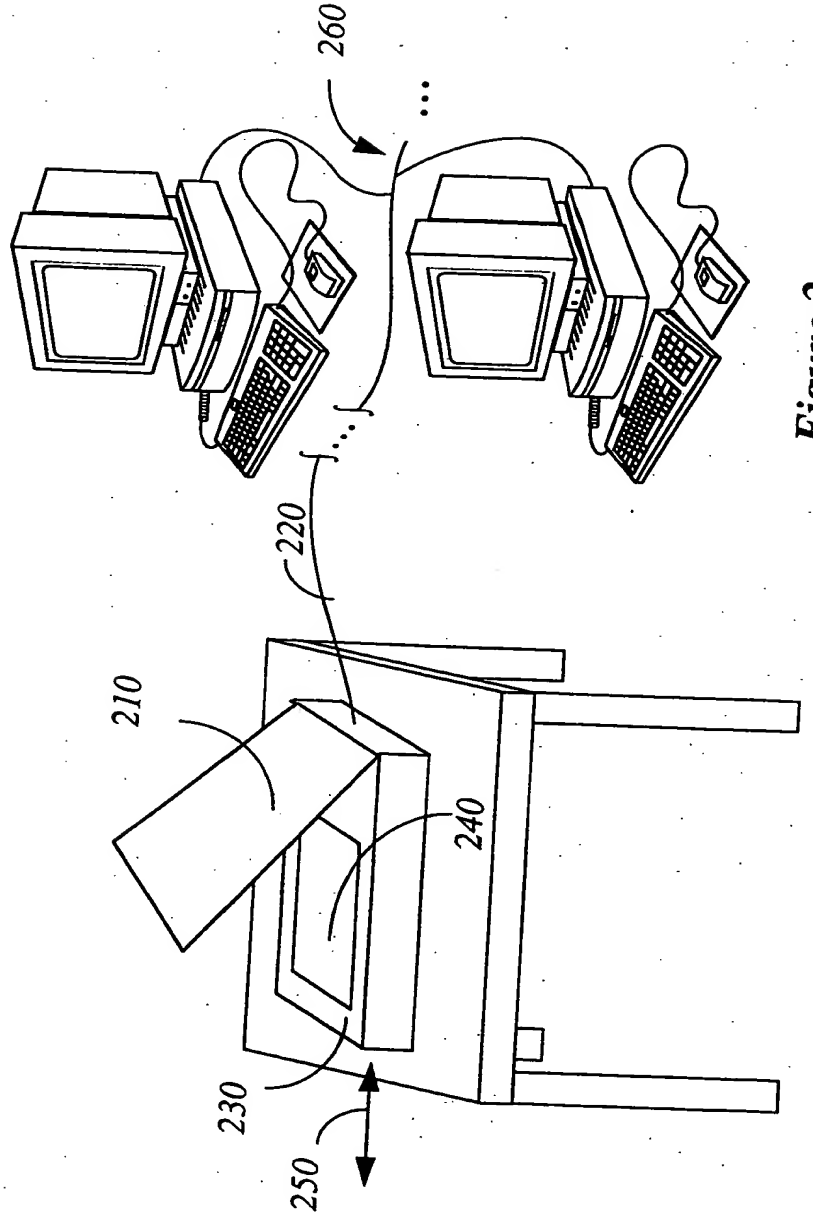


Figure 2

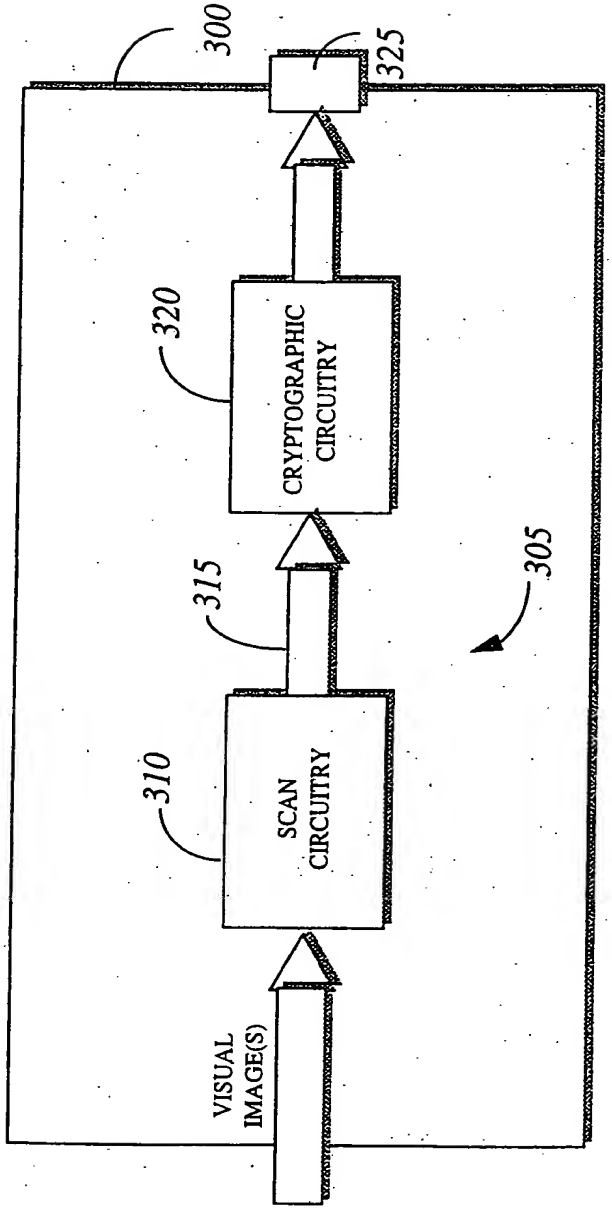

300
325
320
CRYPTOGRAPHIC CIRCUITRY
315
305
310
SCAN CIRCUITRY
VISUAL IMAGE(S)

Figure 3

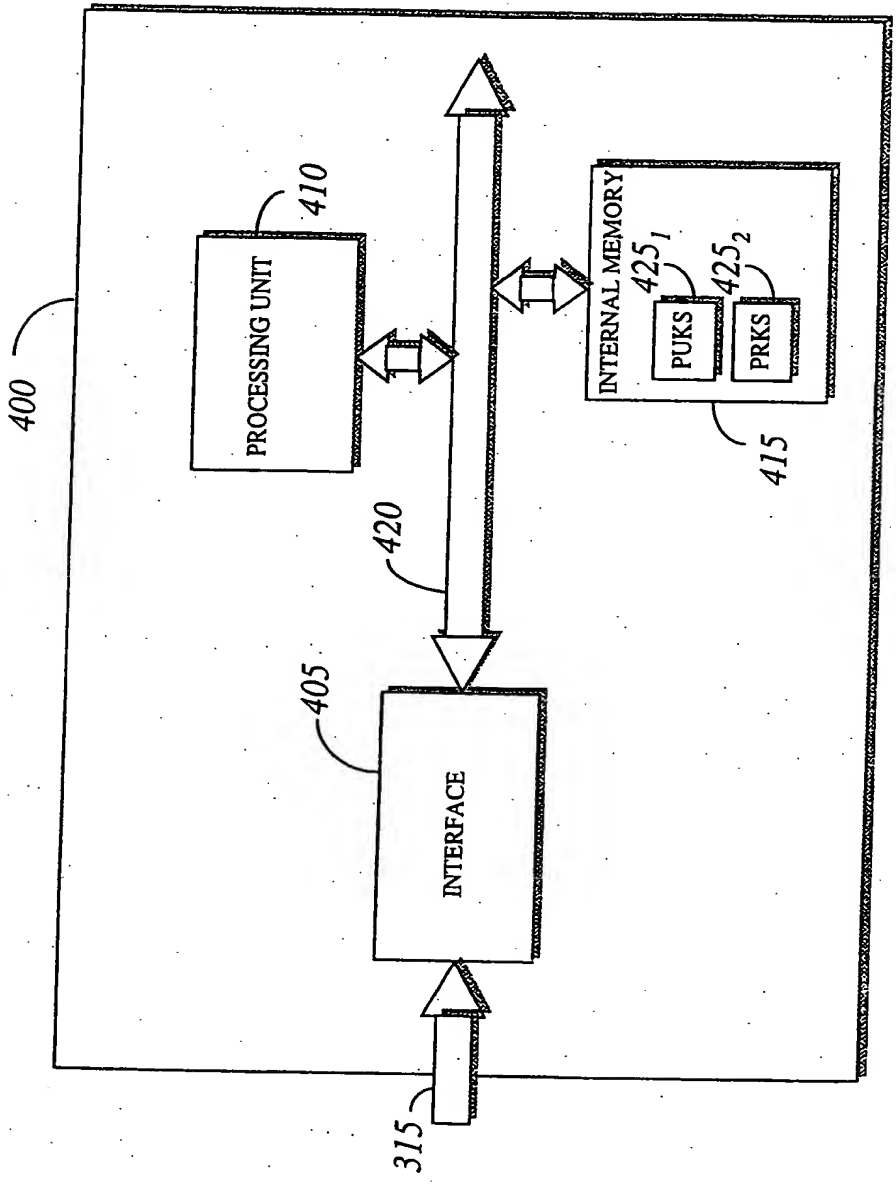

400
PROCESSING UNIT
410
INTERNAL MEMORY
425 1
425 2
PUKS
PRKS
415
420
405
INTERFACE
315

Figure 4

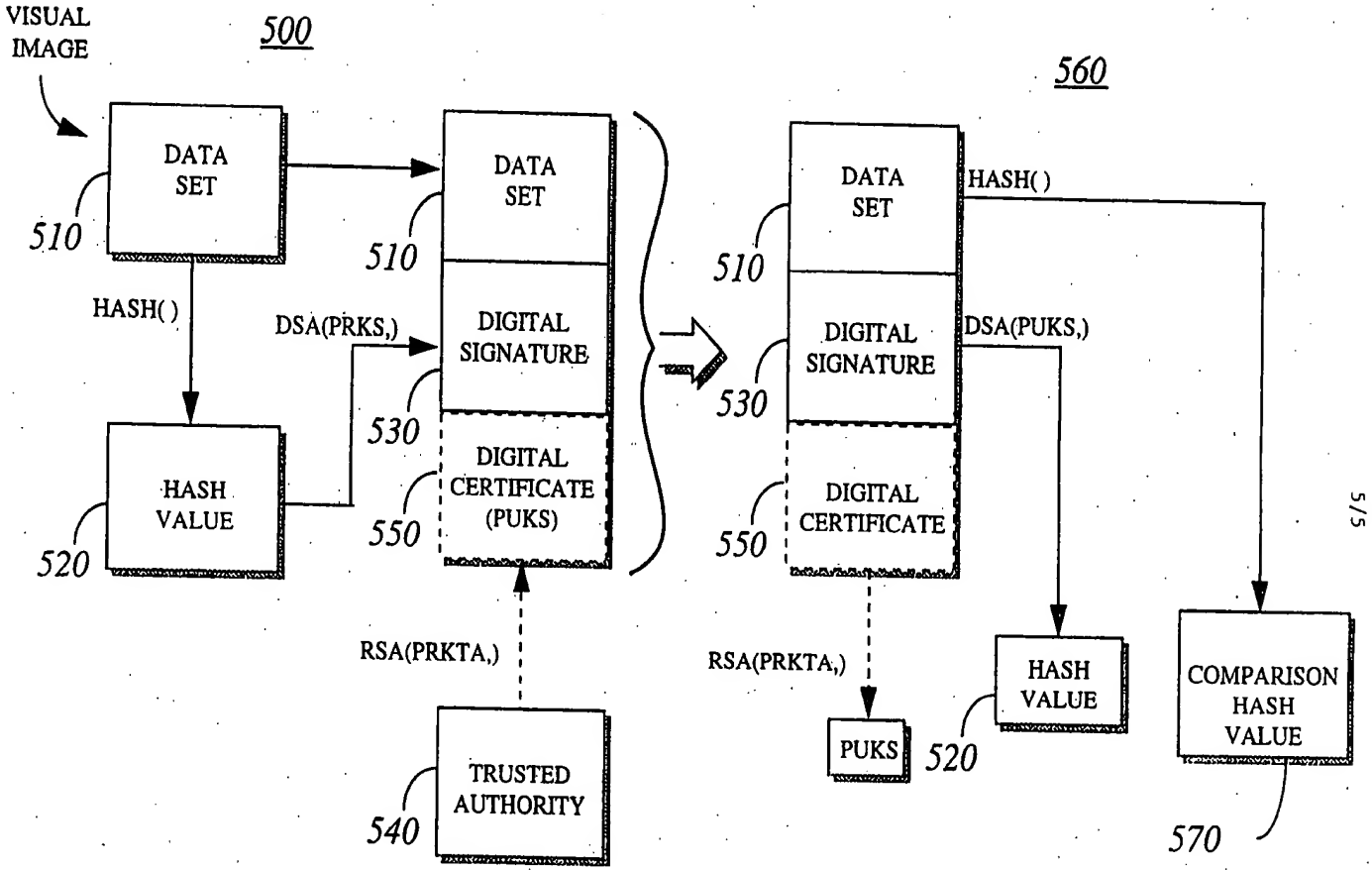

VISUAL IMAGE
500
560
DATA SET
510
HASH( )
HASH VALUE
520
DSA(PRKS,)
DIGITAL SIGNATURE
530
DIGITAL CERTIFICATE (PUKS)
550
RSA(PRKTA,)
TRUSTED AUTHORITY
540
DATA SET
510
HASH( )
DIGITAL SIGNATURE
530
DSA(PUKS,)
DIGITAL CERTIFICATE
550
RSA(PRKTA,)
PUKS
HASH VALUE
520
COMPARISON HASH VALUE
570

Figure 5